IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Anthony L. Fontaine *et al.*	**Examiner:**	Bayat, Bradley B
Application No.:	10/033,716	**Group Art Unit:**	3621
Filing Date:	December 27, 2001	**Office Action Date:**	March 13, 2006
Docket No.	10407-559	**Confirmation No.**	8636
Title: REMOTE ACCESS VERIFICATION ENVIRONMENT SYSTEM AND METHOD		**Customer No.**	30076

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

This amendment is filed in response to the final Office action of March 13, 2006, and is timely filed with a one-month extension of time.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 13 of this paper.

INTRODUCTORY COMMENTS

Claims 1-21, 23, 24, 26-68, and 70-76 are pending in the present application. Claims 1-21, 23, 24, 26-68, 70-76 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Goertzel *et al.* (U.S. Patent No. 6,308,273) in view of Mark (U.S. Patent No. 5,732,133). Claims 22, 25, and 69 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Goertzel *et al.* No claims have been added or canceled. Applicants respectfully request reconsideration of the rejected claims. Applicants respectfully contend that the differences between the claimed invention and the cited references are such that the claimed invention is patentably distinct over the cited references.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A system for enabling remote access to an application server, upon authentication of a location from which a user has sought access as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, the system comprising:

an access server, for receiving and processing a request for access to the application server from a user request enabling means, the server adapted to be located remote from the user's location;

an authenticator for authenticating the location of the user responsive to receipt of a processed request from the access server, the authenticator adapted to be connected to the access server;

means for interconnecting the access server and the authenticator; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location.

2. (original) The system of claim 1, wherein the authenticator comprises an authenticating server.

3. (original) The system of claim 1, wherein the authenticator includes means for determining the identity of the user.

4. (original) The system of claim 1, further comprising means for insuring the user's presence at the location.

5. (original) The system of claim 1, further comprising means for enabling the user to request remote access to the application server.

6. (original) The system of claim 1, wherein the interconnecting means comprise a network.

7. (original) The system of claim 2, wherein the authenticating server includes a database of authorized locations, for enabling verification of the location of the user as an authorized user location.

8. (original) The system of claim 2, wherein the authenticating server comprises a Remote Access Dial-In User Service (RADIUS) server.

9. (original) The system of claim 3, wherein the user identity determining means comprise a challenge and response system.

10. (original) The system of claim 4, wherein the user presence insuring means comprise a card for identifying the user, and a reader for reading the user identifying card, adapted to be connected to the user access request enabling means at the user location.

11. (original) The system of claim 5, wherein the user request enabling means comprise an interface station.

12. (original) The system of claim 5, wherein the user request enabling means comprise a client.

13. (original) The system of claim 5, wherein the user request enabling means include a location identifier.

14. (original) The system of claim 5, wherein the authenticating means are adapted to issue a security challenge to the user request enabling means, and the user request enabling means are further adapted to interrogate the security challenge, to generate a response, and to transmit the response to the authenticator.

15. (original) The system of claim 5, wherein the user request enabling means include an identifier associated with the user's location, and the authenticator comprises means for authenticating the identifier associated with the user's location.

16. (original) The system of claim 5, wherein the user request enabling means include a dialer, located at the user's location, and wherein the dialer includes a number associated therewith.

17. (original) The system of claim 5, wherein the user request enabling means comprise a plurality of user request enabling means, and the interconnecting means comprise a network comprising an intranet which includes at least one local area network, adapted to interconnect at least one of the plurality of user request enabling means and the access server.

18. (original) The system of claim 5, wherein the interconnecting means are further adapted to interconnect the user request enabling means.

19. (original) The system of claim 6, wherein the network comprises an intranet.

20. (original) The system of claim 6, wherein the network comprises the Internet.

21. (original) The system of claim 8, further comprising means for enabling the user to request remote access to the application server, wherein the authenticating server is further adapted to issue a security challenge to the user request enabling means.

22. (original) The system of claim 15, wherein the locating identifier comprises a cookie.

23. (original) The system of claim 16, wherein the authenticator comprises a number identifier for identifying the number associated with the dialer located at the user's location.

24. (original) The system of claim 16, wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing

therefrom and each dialer associated with a different user location, and the authenticator further comprises means for identifying the first number dialed from in the dialing system.

25. (original) The system of claim 20, wherein the locating identifier comprises a dynamic cookie.

26. (original) The system of claim 21, wherein the user request enabling means are adapted to issue a response to the security challenge, and the authenticating means include a database for enabling verification of the response of the user request enabling means to the security challenge.

27. (original) The system of claim 23, wherein the number identifier comprises Automatic Number Identification.

28. (original) The system of claim 24, wherein the first number identifying means comprises Dialed Number Identification Services.

29. (original) The system of claim 26, wherein the authenticator is further adapted to verify the response of the user request enabling means to the security challenge based on the database in the authenticator, and to authorize access to the application server.

30. (currently amended) A system for enabling remote access to an application server, upon authentication of a location from which a user has sought access as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, the system comprising:

an access server, for receiving and processing a request for access to the application server from a user request enabling means, the server adapted to be located remote from the user's location;

an authenticator for authenticating the location of the user responsive to receipt of the processed request from the access server, the authenticator adapted to be connected to the access server, the authenticator including a Remote Access Dial-In Service (RADIUS) server;

means for interconnecting the access server and the authenticator;

means for enabling the user to request remote access to the application server, such means including a dialer, located at the user's location, wherein the dialer includes a dialing number associated therewith; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location.

31. (original) The system of claim 30, wherein the authenticator includes a number identifier for identifying the number associated with the dialer located at the user's location.

32. (original) The system of claim 30, and further comprising a dialing system including a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user location, and the authenticator comprises means for identifying the first number dialed from the dialing system.

33. (original) The system of claim 31, wherein the number identifier comprises Automatic Number Identification.

34. (original) The system of claim 32 wherein the first number identifying means comprises Dialed Number Identification Services.

35. (currently amended) A system for enabling remote access to an application server, upon authentication of a location from which a user has sought access as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, comprising:

an access server, for receiving a request for access to the application server from user request enabling means, adapted to be located remote from the user's location;

an authenticator for authenticating the location of the user, the authenticator adapted to be connected to the access server and further including an identifier for determining the identity of the user;

means for interconnecting the access server and the authenticator;

means for enabling the user to request remote access to the application server; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a location other than the user location.

36. (original) The system of claim 35, wherein the user identifier further comprises a challenge and response system.

37. (original) The system of claim 35, wherein the authenticator is adapted to issue a security challenge to the user request enabling means, and the user request enabling means are further adapted to interrogate the security challenge, to generate a response, and to transmit the response to the authenticator.

38. (original) The system of claim 35, further comprising means for enabling the user to request remote access to the application server, wherein the authenticator server is further adapted to issue a security challenge to the user request enabling means.

39. (original) The system of claim 38, wherein the user request enabling means are adapted to issue a response to the security challenge, and the authenticator includes a database for enabling verification of the response of the user request enabling means to the security challenge.

40. (original) The system of claim 39, wherein the authenticating means are further adapted to verify the response of the user request enabling means to the security challenge based on the database in the authenticator, and to authorize access to the application server.

41. (currently amended) A system for enabling remote access to an application server upon authentication of a location from which a user has sought access as an authorized location for enabling access to the application server and processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, comprising:

an access server, for receiving a request for access to the application server from user request enabling means adapted to be located remote from the user's location;

an authenticator for authenticating the location of the user, adapted to be connected to the access server;

means for interconnecting the access server and the authenticator;

means for insuring user's presence at the location; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location.

42. (original) The system of claim 41, wherein the user presence insuring means comprise a card for identifying the user and a reader for reading the user identifying card, adapted to be connected to the user access request enabling means at the user location.

43. (currently amended) A system for enabling remote access to an application server, upon authentication of a location from which a user has sought access thereto as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, comprising:

an access server, for receiving and processing a request for access to the application server from user request enabling means, the server adapted to be located remote from the user's location;

an authenticating server for authenticating the location of the user responsive to receipt of the processed request from the access server, adapted to be connected to the access server;

a network for interconnecting the access server and the authenticating server; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location.

44. (original) The system of claim 43, further comprising a client for enabling the user to request remote access to the application server.

45. (original) The system of claim 43, wherein the authenticating server includes a database of authorized locations, for enabling verification of the location of the user as an authorized user location.

46. (original) The system of claim 44, wherein the client includes an identifier associated with the user's location, and the authenticating server is adapted to authenticate the identifier associated with the user's location.

47. (original) The system of claim 44, wherein the client comprises a plurality of clients and the network comprises an intranet which includes a plurality of local area networks, each adapted to interconnect at least one of the plurality of clients and the access server.

48. (currently amended) A method of enabling remote access to an application server, upon authentication of a location from which a user has sought access thereto as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, in a system which comprises an access server, for receiving and processing a request for access to the application server from user request enabling means, adapted to be located remote from the user's location, an authenticator for authenticating the location of the user responsive to receipt of the processed request from the access server, adapted to be connected to the access server, and means for interconnecting the access server and the authenticator, wherein the method comprises:

requesting an access server to enable a user at a user's location to access an application server;

authenticating the location of the user in the authenticator; and

identifying a first number from which the user has dialed, wherein a first number authenticating system provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location; and

determining in the authenticator whether to enable the user to access the application server based on the authenticating of the user's location.

49. (original) The method of claim 48, wherein the authenticator comprises an authenticating server, and wherein authenticating further comprises authenticating through the authenticating server.

50. (original) The method of claim 48, wherein the authenticator includes means for determining the identity of the user, and wherein authenticating further comprises determining the identity of the user through the user identity determining means.

51. (original) The method of claim 48, further comprising insuring the user's presence at the location through a user presence insuring means.

52. (original) The method of claim 48, further comprising enabling the user to request remote access to the application server through the user request enabling means.

53. (original) The method of claim 48, further comprising interconnecting the access server and the authenticating means through a network.

54. (original) The method of claim 49, wherein authenticating comprises authenticating through an authorized location database.

55. (original) The method of claim 49, wherein authenticating further comprises authenticating through a RADIUS server.

56. (original) The method of claim 50, wherein determining further comprises challenging the identity of the user and processing the response thereto.

57. (original) The method of claim 51, wherein insuring further comprises reading a user identifying card which identifies the user, via a card reader, connected to the user access request enabling means at the user location.

58. (original) The method of claim 52, wherein enabling further comprises enabling the user request through an interface station.

59. (original) The method of claim 52, wherein enabling further comprises enabling the user request through a client.

60. (original) The method of claim 52, wherein enabling further comprises enabling the user request through the location identifier.

61. (original) The method of claim 52, further comprising issuing a security challenge from the authenticator interrogating a security challenge, generating a response to the challenge, and transmitting the response from the user request enabling means.

62. (original) The method of claim 52, wherein authenticating comprises authenticating the user's location through a user associated identifier.

63. (original) The method of claim 52, wherein enabling comprises enabling through a dialer having an associated number.

64. (original) The method of claim 52, wherein interconnecting comprises interconnecting a plurality of user request enabling means through a plurality of local area networks.

65. (original) The method of claim 52, wherein interconnecting further comprises interconnecting with a user request enabling means.

66. (original) The method of claim 53, wherein the network comprises an intranet, and wherein interconnecting further comprises interconnecting through the intranet.

67. (original) The method of claim 53, wherein the network comprises the Internet, and wherein interconnecting further comprises interconnecting through the Internet.

68. (original) The method of claim 55, wherein authenticating further comprises issuing a security challenge to the user request enabling means through an authenticating server.

69. (original) The method of claim 62, wherein authenticating further comprises authenticating through a locating identifier cookie.

70. (original) The method of claim 63, wherein the authenticator comprises means for identifying the number associated with the dialer located at the user's location, and

wherein the step of authenticating further comprises identifying the number associated with the dialer.

71. (original) The method of claim 63 wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user location, and the authenticator comprises means for identifying the first number dialed in the dialing system, and wherein the step of authenticating further comprises identifying the first number dialed.

72. (original) The method of claim 67, wherein the locating identifier comprises a dynamic cookie.

73. (original) The method of claim 68, wherein the user request enabling means are adapted to issue a response to the security challenge, and the authenticator include a database for enabling verification of the response of the user request enabling means to the security challenge, and wherein the step of authenticating further comprises verifying the response to the security challenge through the verification database.

74. (original) The method of claim 70, wherein identifying further comprises identifying through Automatic Number Identification.

75. (original) The method of claim 71, wherein the step of identifying further comprises identifying through Dialed Number Identification Services.

76. (original) The method of claim 73, wherein the authenticator is further adapted to verify the response of the user request enabling means to the security challenge based on the database in the authenticator, and to authorize access to the application server, and further comprising the step of authorizing access to an application server.

REMARKS

In response to the Office Action mailed March 13, 2006, the Examiner's claim rejections have been considered. Applicants have fully considered the references (Goertzel *et al.* and Mark) as potentially teaching all or part of the claimed invention. Applicants have also considered the context of the passage taught by the references as cited by the Examiner. As such, the Applicants' response is not directed to a specific portion of the cited reference, but rather to the reference as a whole. Applicants respectfully traverse all rejections regarding all pending claims and earnestly solicit allowance of these claims.

1. Claim Rejection 35 U.S.C. § 103(a) – Claims 1-21, 23, 24, 26-68, and 70-76

Claims 1-21, 23, 24, 26-68, and 70-76 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Goertzel *et al.* (U.S. Patent No. 6,308,273) in view of Mark (U.S. Patent No. 5,732,133). Applicants respectfully traverse this rejection. For brevity, only the bases for the rejection of the independent claims are traversed in detail on the understanding that the dependent claims are also patentably distinct over the prior art, as they depend directly from their respective independent claims. Nevertheless, the dependent claims include additional features that, in combination with those of the independent claims, provide further, separate, and independent bases for patentability.

Applicants respectfully submit that Goertzel and Mark, alone or in combination, do not teach, suggest, or disclose a system for enabling remote access to an application server that includes "a first number authentication system that provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location." More specifically, the first number authentication system prevents a person from attempting to gamble in an unauthorized jurisdiction by calling or forwarding calls to a venue that does allow gambling and falsely originating the call from such venue. For example, the number authentication system prevents a user, located in California, from originating a call in California to a phone number in Nevada, and then using the Nevada phone number to place a wager at a Nevada casino.

As noted by the Examiner, Goertzel does not teach or disclose a number authentication mechanism providing anti-circumvention protection. Additionally, Applicants respectfully submit that the Mark reference does not make up for this deficiency. The Mark reference merely teaches and discloses a system for selecting and generating telephone access numbers for limiting access to long distance telephone service. That is, Mark teaches a secured system having a handheld auto-dialer that is capable of accessing long distance telephone service. The system includes a system clock and a plurality of telephone access numbers, each of which is capable of accessing the telephone service at a randomly selected time. Mark teaches that unauthorized access of telephone services by using an invalid number causes the telephone system to inhibit the completion of the call and then traces the call to determine the origin of the offending call.

However, Applicants submit that the Mark system does not provide any anti-circumvention protection. While the Mark reference teaches that a call may be traced, Applicants submit that the Mark reference does not teach how an unauthorized call may be traced through multiple numbers. Referring back to the previous example, the system in Mark may determine that the phone number in Nevada was used to access the telephone system, but the Mark telephone system would not be able to determine that the call in Nevada was originated from a phone number located in California. As such, Applicants submit that the Mark reference would not be able to determine that the caller was actually located in California, rather than Nevada, since the Mark reference is silent as to the use of any anti-circumvention technology used to trace a phone number. In short, Mark does not teach the use of anti-circumvention protection based upon physical location because this reference is not directed to solving the problem of people accessing a system from an unauthorized jurisdiction. Rather, the Mark reference is focused on preventing individuals from hacking into a telephone system and making unauthorized long distance phone calls (i.e., theft of long distance services). In sharp contrast, the claimed invention is directed to preventing a person from remotely accessing a gambling system from an unauthorized jurisdiction.

Moreover, Applicants submit that there is no motivation to combine the Goertzel and Mark references. "The reason, suggestion, or motivation to combine [prior art references] may be found explicitly or implicitly: 1) in the prior art references themselves; 2) in the knowledge of

those of ordinary skill in the art that certain references, or disclosures in those references are of special interest or importance in the field; or 3) from the nature of the problem solved, 'leading inventors to look to references relating to possible solutions to that problem.'" Ruiz v. AB. Chance Co., 234 F.3d 654,6654 (Fed. Cir. 2000) (quoting Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc., 75 F.3d 1568, 1572 (Fed. Cir. 1996)).

As the Examiner points out, the Goertzel reference does not disclose a number authentication system providing anti-circumvention protection. Accordingly, there is no motivation to combine these references because these references are directed to solving problems different from the claimed invention. The Goertzel reference is directed to solving the problem of unauthorized access to a secured network based upon the user's connection type or communication link to the network. The Mark reference is directed to solving the problem of unauthorized access to telephone services. More specifically, the Mark reference teaches a handheld auto-dialer and related system that "encrypts calling card and other data...by selectively altering pre-selected characteristics of a DTMF tone sequence." (See, col. 5, line 66-col. 6, line 7).

Applicants submit that these references are directed to solving problems very different from each other, as well as, being different from the claimed invention. The Goertzel reference is directed to restricting access to a secured server based upon the type of user connection. The Mark reference is directed to preventing unauthorized access to telephone services by an unauthorized user (i.e., theft of services). In contrast, the claimed invention is directed to ensuring that an authorized user is in a physical location (within a legal jurisdiction) that allows remote gambling. A person of ordinary skill in the art would not look to the Mark reference for anti-circumvention technology related to physical location. That is, Mark does not teach that access to remote services may be restricted based upon physical location.

Because the Goertzel and Mark references fail to teach or suggest all of the claimed elements, Applicants respectfully request the rejection be withdrawn. Accordingly, Applicants respectfully submit that the 35 U.S.C. § 103(a) rejection of claims 1-21, 23, 24, 26-68, and 70-76 has been overcome.

2. Claims Rejections - 35 U.S.C. §103(a) – Claims 22, 25, and 69

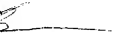
Claims 22, 25, and 69 stand rejected as being unpatentable over Goertzel *et al.* (U.S. Patent No. 6,508,710). According to a teleconference with the Examiner on November 21, 2005, U.S. Patent No. 6,508,710 was improperly cited. Rather, the rejection is based on Goertzel *et al.* (U.S. Patent No. 6,308,273) and Mark (U.S. Patent No. 5,732,133). Applicants respectfully traverse this rejection. In light of the arguments submitted in Section I of this response, Applicants submit that the dependent claims 22, 25, and 69 are not obvious in view of Goertzel and Mark, because these references, alone or in combination, fail to teach, suggest, or disclose "a number authentication system that provides anti-circumvention protection that prevents activation of a dialer from a physical location other than the user location." Moreover, the dependent claims include additional features that, in combination with those of the independent claims, provide further, separate, and independent bases for patentability. Accordingly, the Applicants respectfully submit that the 35 U.S.C. § 103(a) rejection of claims 22, 25, and 69 as unpatentable over Goertzel and Mark has been overcome.

CONCLUSION

Applicants have made an earnest and *bona fide* effort to clarify the issues before the Examiner and to place this case in condition for allowance. In view of the foregoing discussions, it is clear that the differences between the claimed invention and the cited references are such that the claimed invention is patentably distinct over the cited references. Therefore, reconsideration and allowance of all of claims 1-21, 23, 24, 26-68 and 70-76 are believed to be in order, and an early Notice of Allowance to this effect is respectfully requested. If the Examiner should have any questions concerning the foregoing, the Examiner is invited to telephone the undersigned attorney at (310) 712-8323. The undersigned attorney can normally be reached Monday through Friday from about 9:30 AM to 6:30 PM Pacific Time.

Respectfully submitted,

Date: June 14, 2006



Andrew B. Chen
Reg. No. 48,508
BROWN RAYSMAN MILLSTEIN FELDER & STEINER LLP
1880 Century Park East, 12th Floor
Los Angeles, CA 90067-1621
(310) 712-8323 telephone
(310) 712-8383 facsimile